

## Benefits

### Protected Applications Execution Environment

Custom Java applications are installed within protected execution areas to isolate application code from system code. Applications executed within this protected environment can only access Luna SP's integrated HSM through a policy layer separating the application from the HSM. Signed Code Prevents Unauthorized Execution. Applications are digitally signed to ensure that only customer-trusted code can be loaded and executed on the Luna SP. As applications cannot be altered without invalidating the signatures, the code signing process ensures the logical integrity of the security appliance.

### Standard Tools for Rapid Development

Luna SP supports the J2S development environment and is pre-populated with standard tools to simplify application development. A Web server, SOAP stack, and J2SE compliant XML Web service container are preinstalled and optimized to support XML and Web Services applications running on Luna SP. Custom applications can be developed quickly and easily, simplifying design and testing, shortening development cycles, and eliminating the need for proprietary development funds.

### Maximum Application and Cryptographic Performance

Applications running on Luna SP take advantage of a streamlined appliance platform with the minimal set of services. This reduces system overhead and maximizes application performance. Luna SP's integrated K3 Cryptographic Engine is capable of up to 7,000 transactions per second to eliminate cryptographic processing bottlenecks.

# Luna® SP 2.0

## Network-Attached Hardware Security Module

Luna SP allows developers to securely deploy web applications, web services, and other Java applications in a protected hardened security appliance.



### Deploy Secure Applications Anywhere with Ease

Luna SP is designed for reliable deployment of security applications anywhere on your network. Luna SP leverages standard Java development tools to simplify development of custom applications and reduce integration and testing cycles. Its programmability and security make it easy to develop custom applications, integrate them into an appliance, and deploy them securely in a very short time. Enterprises deploying security applications can streamline development processes, eliminate hardware duplication, and reduce ongoing operational costs with Luna SP.

### The Programmability of an Application Server with the security of an HSM

Luna SP provides a secure platform for the deployment of web applications, web services, and Java applications that require the highest levels of trust by combining a standard application server platform and a dedicated Hardware Security Module (HSM) within a single security appliance. The Luna SP's application server is security hardened and optimized to take advantage of the integrated HSM and its specialized hardware features.

### Protected Application Environment

Applications installed on Luna SP execute within a protected application container to ensure that application code and system code are isolated. Applications executing within this trusted environment have exclusive

access to the Luna SP integrated HSM through a policy layer separating the application from the HSM.

### Secures Applications and their Cryptographic keys

Luna SP increases application security by providing a trusted execution environment that protects an application's sensitive software components and cryptographic keys from physical, logical, and operational threats. Customer-provided application code is digitally signed and securely installed on the Luna SP to assure code integrity and prevent the execution of unauthorized applications.

Luna SP 2.0 features an integrated FIPS 140-2, Level 3 validated HSM that provides hardware protection for cryptographic keys and processes.

### Auditability, Authentication, and Policy Control

Luna SP combines proven hardware key management with rigorous logging features to provide non-repudiable audit records of access and cryptographic key usage. Split administrative roles, including M of N multi-person authentication, and flexible security policy management, maintain tight control over sensitive administrative functions, including code loading and management of cryptographic keys.

### Tamper-Protected Hardware

Integrated physical security measures include tamper-evident seals, intrusion detection switches, and shielded connectors designed to resist physical attacks.





FIPS 140-2 Validated	✓	In Progress
RoHS Compliant		✓
2U Rackmount Chasis	* ✓	
1U Rackmount Chasis		
Transactions Per Second	>1200	3000/7000**
Cyrptographic APIs		
ECC	✓	✓
ECDSA		✓
JRE 1.5		✓
PED	✓	✓
PED II	✓	✓

\* Can upgrade the Luna SP 1.5 to the 2.0 functionality

\*\* Still in testing

## Simplified Administration

Luna SP features a Secure Command Line Interface to simplify remote system administration and streamline maintenance. A local console port is offered for initial configuration or direct system administration

## Two-Factor Administrative

Luna SP uses two-factor, trusted path authentication with the Luna PED (PIN Entry Device), a handheld authentication console, to control access to HSM administration functions and applications.

## Ethernet-Attached for Flexibility

Luna SP connects to standard TCP/IP (Internet Protocol) networks to ensure ease of deployment into existing network infrastructure. Two Ethernet interfaces with integrated firewalls can be used for services or administrative access.



## NORDIC DISTRIBUTOR

### PERICO AS

Lilleakerveien 4, Inngang 1A  
0283 OSLO  
NORWAY

Email: info@perico.no  
Tel: +47 22 06 40 50  
www.pericosecurity.com

## Technical Specifications

### Java Service Environment

Luna SP includes the following tools to support custom Java services:

- Java J2SE (JVM)
- Xerces (XML parsing)
- Apache Tomcat (Application and Webserver)
- Apache Axis (SOAP)

### Cryptographic APIs

- JCE/JCA

### Hardware Validations

- FIPS 140-2 Level 3 validated - certificate number 375
- RoHS compliant certificate number

### Cryptographic Performance

Luna SP 1.5 – Over 1200 1024-bit RSA cryptographic operations per second  
Luna SP 2.0 – 3000 & 7000 tps

### Cryptographic Algorithms

#### Asymmetric Key

- Diffie-Hellman (1024-4096 bit) RSA (512-4096 bit)

#### Digital Signing

- RSA (1024-4096 bit), DSA (512-1024 bit)

#### Symmetric Keys

- 3DES, AES, RC2, ARC4, RC5

#### Hash Digest

- SHA-1, SHA-2, (160, 256, 512), MD-5

#### Message Authentication Codes (MAC)

- HMAC-MD5, HMAC-SHA-1, SSL3-MD5-MAC, SSL3-SHA-1-MAC

### Physical Characteristics

#### Connectivity

- 2x 10/100 Ethernet, CAT5, UTP Local administration serial console port

#### Dimensions

- 2U full-length 19" rackmount chassis (ANSI/EIA-310-D compliant)
- 19.0" x 20.6" x 3.45" (482.6mm x 523.2mm x 87.7mm)
- 35lb (15.9kg)
- 1U full-length 19" rackmount chassis (Luna SA 4.0 model) (ANSI/EIA-310-compliant)

#### Power Requirements

- 1.5A@120V Max

#### Temperature

- Operating 0°C to 40°C,
- Storage -20°C to +65°C

### Regulatory Standards

#### Certification

- U/L 1950 (EN60950) & CSA C22.2 compliant
- FCC Part 15 - Class B
- ISO - 9002 Certification

